WHAT IS CLAIMED IS:

1. In a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising:

(a) a processor located within the digital camera for producing a public/private key pair; and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature.

2. The digital camera claimed in claim 1, wherein the processor includes means for producing a random seed for the private key by hashing an initial test image captured by the digital camera.

3. The digital camera according to claim 2, further including:

(i) a shutter and an image sensor for capturing images;

(ii) a variable gain amplifier coupled to the image sensor;

(iii) an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images; and

(iv) the processor causing the variable gain amplifier to be in a high gain condition when the initial test image is captured.

4. The digital camera claimed in claim 1, wherein the processor includes one or more algorithms for producing a random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing.

5. The digital camera claimed in claim 4, wherein the processor includes an image processing algorithm which uses JPEG compression.

6. In a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera, the improvement comprising the steps of:

(a) producing the private key in the digital camera; and

(b) storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image.

7. A method of authenticating an image captured by a digital camera, comprising the steps of:

(a) producing a private key/public key pair in the digital camera;

(b) storing the private key in a memory in the digital camera;

(c) communicating the public key to a user;

(d) capturing a digital image;

(e) hashing the captured digital image in the digital camera to produce an image hash;

(f) encrypting the image hash in the digital camera with the private key to produce a digital signature; and

(g) authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

8. A method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of:

(a) manufacturing a digital camera with an internal processor for processing a public/private key pair, storing the public key in a memory in the digital camera and communicating the public key to a camera operator;

(b) sending the digital camera to an authentication service;

(c) activating the digital camera at the authentication service to produce the public/private key pair, and registering the public key at the authentication service; and

(d) sending the digital camera to a user.

9. In a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values, the improvement comprising:

(a) a processor located within the digital camera for producing a public/private key pair; and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature and the metadata signature.

10. A method of producing an image authentication signature in a digital camera, comprising the steps of:

(a) capturing a digital image;

(b) compressing the captured digital image;

(c) providing one or more metadata values;

(d) hashing the compressed captured digital image and at least one of the metadata values to produce an image hash; and

(e) encrypting the image hash to produce the image authentication signature.

11. The method according to claim 10 further including the step of storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values.

12. The method according to claim 10 wherein the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature.

13. The method according to claim 10 further including the steps of:

producing a public/private key pair in the digital camera;

storing the private key in a memory in the digital camera;

wherein the encrypting step includes encrypting the image hash with the private key to produce the image authentication signature; and

authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

14. The method according to claim 10 further including the steps of: hashing the uncompressed captured digital image to produce a random number *k*; and wherein the encrypting step includes using the random number *k* to produce the image authentication signature.

15. The method according to claim 10 wherein the encrypting step further produces a metadata signature corresponding to the one or more metadata values.